Provision Certificates to iOS Devices

Technical Note

Provision Certificates to iOS Devices Technical Note

June 26, 2012

04-500-171341-20120626

Copyright© 2012 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2012-06-26	Initial release.

Introduction

The purpose of this document is to provide instructions on how to install the required certificates for FortiClient for iOS devices.

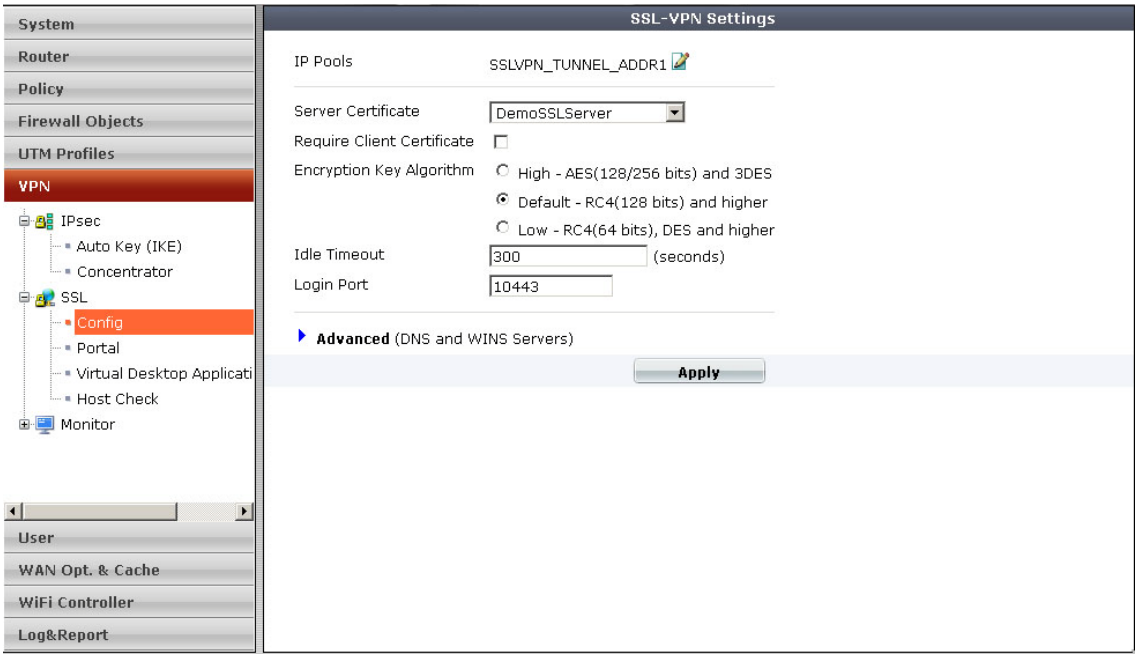
Provision Certificates to iOS Devices

Server certificate

The following option is available for the *Server Certificate* on the FortiGate:

- CA signed certificate

Figure 1: FortiGate Server Certificate



If the *Server Certificate* is configured with a CA signed certificate, the certificate needs to be installed on the iOS device before the FortiClient application can be used to establish the SSL-VPN connection.

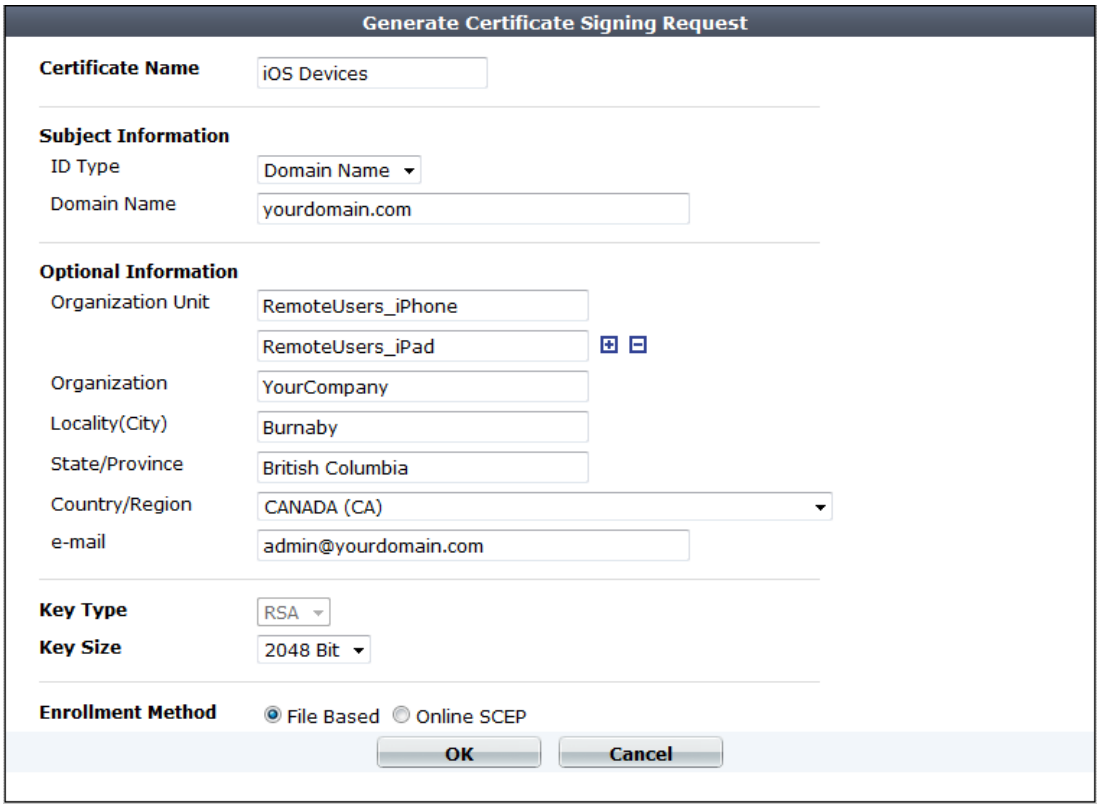
Generate a new certificate from the FortiGate device

You can generate a certificate request file, based on the information you enter to identify the FortiGate unit. Certificate request files can then be submitted for verification and signing by a certificate authority (CA).

To generate a certificate request

1. Go to *System* > *Certificates* > *Local Certificates*
2. Select *Generate* from the menu pane
3. Configure the following information:

Figure 2: Generate Certificate Signing Request



Certificate Name	Enter a unique name for the certificate request.
Subject Information	Information that the certificate is required to contain in order to uniquely identify the FortiGate unit. **ID Type** Select which type of identifier will be used in the certificate to identify the FortiGate unit: • Host IP • Domain Name • E-Mail Which type you should select varies by whether or not your FortiGate unit has a static IP address, a fully-qualified domain name (FQDN), and by the primary intended use of the certificate. *Host IP* requires that the FortiGate unit has a static, public IP address. It may be preferable if clients will be accessing the FortiGate unit primarily by its IP address. *Domain Name* requires that the FortiGate unit has a fully qualified domain name (FQDN). It may be preferable if clients will be accessing the FortiGate unit primarily by its domain name. *E-Mail* does not require either a static IP address or a domain name. It may be preferable if the FortiGate unit does not have a domain name or public IP address. **IP** Enter the static IP address of the FortiGate unit. This option appears only if ID Type is Host IP. **Domain Name** Type the fully-qualified domain name (FQDN) of the FortiGate unit. The domain name must resolve to the static IP address of the FortiGate unit or protected server. This option appears only if ID Type is Domain Name. **E-Mail** Type the email address of the owner/admin of the FortiGate unit. This option appears only if ID Type is E-Mail.

Optional Information	Information that you may include in the certificate, but which is not required including: **Organization Unit** Type the name of your organizational unit, such as the name of your department. To enter more than one organizational unit name, click the **+** icon, and enter each organizational unit separately in each field. **Organization** Type the legal name of your organization. **Locality (City)** Type the name of the city or town where the FortiGate unit is located. **State/Province** Type the name of the state or province where the FortiGate unit is located. **Country** Select the name of the country where the FortiGate unit is located. **e-mail** Type an email address that may be used for contact purposes.
Key Type	The type of algorithm used to generate the key. This option cannot be changed, but appears in order to indicate that only RSA is currently supported.
Key Size	Select a security key size of 1024 Bit, 1536 Bit or 2048 Bit. Larger keys are slower to generate, but provide better security.
Enrollment Method	Select either: **File Based**: You must manually download and submit the resulting certificate request file to a certificate authority (CA) for signing. Once signed, upload the local certificate. **Online SCEP**: The FortiGate unit will automatically use HTTP to submit the request to the simple certificate enrollment protocol (SCEP) server of a CA, which will validate and sign the certificate. Enter the CA Server URL and the Challenge Password.

4. Select *OK*

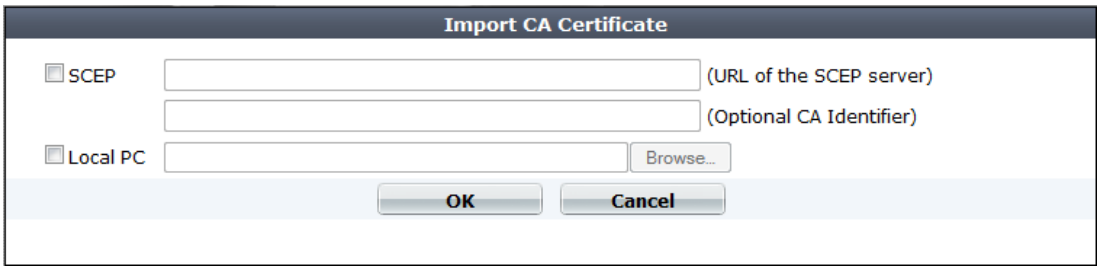
The certificate is generated. If you selected file-based enrollment, you must now download and manually submit the resulting CSR to a CA.

Import the signed CA certificate to the FortiGate device

To import the signed CA certificate to the FortiGate device, follow the steps below.

1. Go to *System* > *Certificates* > *CA* Certificates and select Import from the menu pane.

Figure 3: Import a CA certificate



SCEP	To import using SCEP, select SCEP. Enter the URL of the SCEP server from which to retrieve the CA certificate. Optionally, enter identifying information of the CA, such as the filename.
Local PC	To import from a file, select Local PC, then select Browse and find the location on the management computer where the certificate has been saved. Select the certificate, and then select Open.

2. Select *OK*

The system assigns a unique name to each CA certificate. The names are numbered consecutively (CA_Cert_1, CA_Cert_2, CA_Cert_3, and so on).

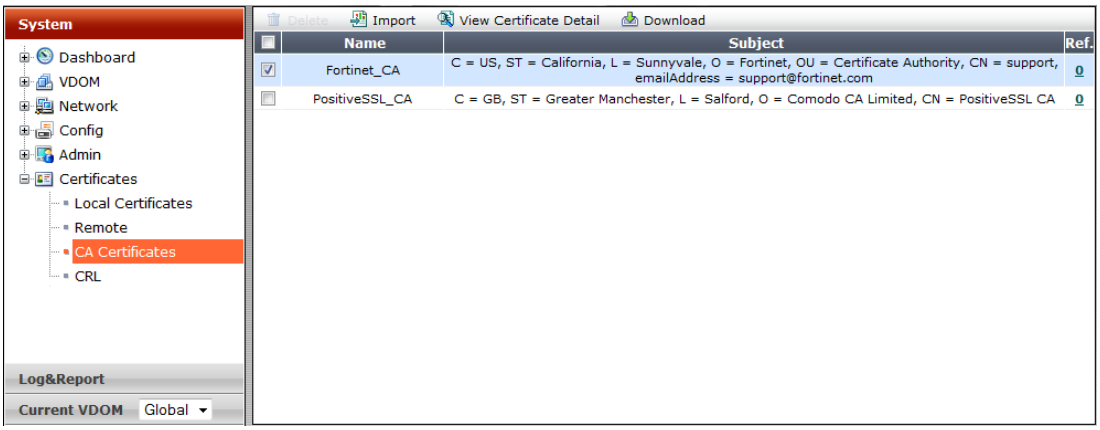
The client needs only the CA certificate, not the server certificate. If the CA certificate is from a trusted root certificate authority that is already supported by iOS 5.0, you do not need to import the CA since it is already on the iOS device.

Download the certificate from the FortiGate device

To download the certificate from the FortiGate device, follow the steps below.

1. Go to *System* > *Certificates* > *CA Certificates* and select the CA certificate from the list.
2. Select *Download* from the menu pane to save the certificate file to your local hard drive.

Figure 4: Download the CA certificate



Distribute the FortiGate CA certificate to iOS devices

You can distribute the CA certificate to iOS devices using:

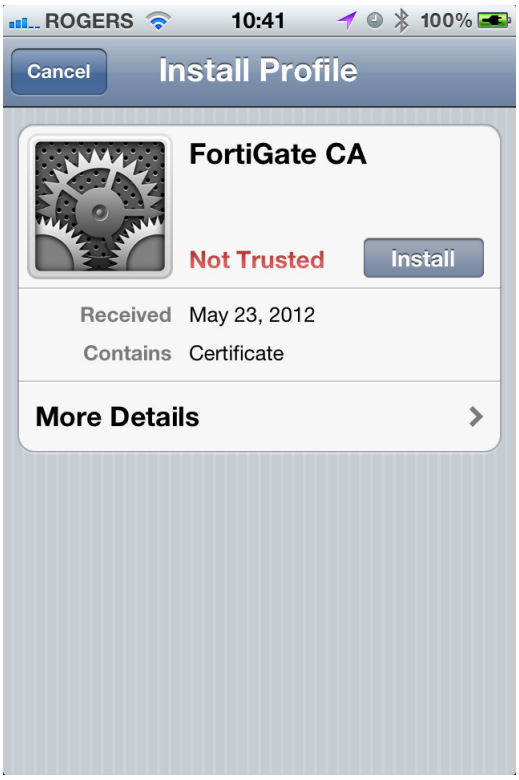
- Mail: the certificate is sent as an attachment to the user
- Safari: the certificate is hosted on a secured website
- iOS Configuration Utility, which is available from Apple
- Simple Certificate Enrollment Protocol (SCEP) for over-the-air distribution.

Install the CA certificate on the iOS device

To install the certificate on the iOS device, follow the steps listed below.

1. The FortiGate administrator mails the CA certificate to the user as an email attachment.
2. The end user opens the email and taps the file name of the attachment.
3. Select *Install* to start the certificate installation.

Figure 5: Install Profile message



4. The following warning message is presented to the end user with information on the *Profile* and *Root Certificate*. Select *Install* to continue with the installation.

Figure 6: Warning message

5. The end user receives the following message to confirm that the certificate has been installed successfully.

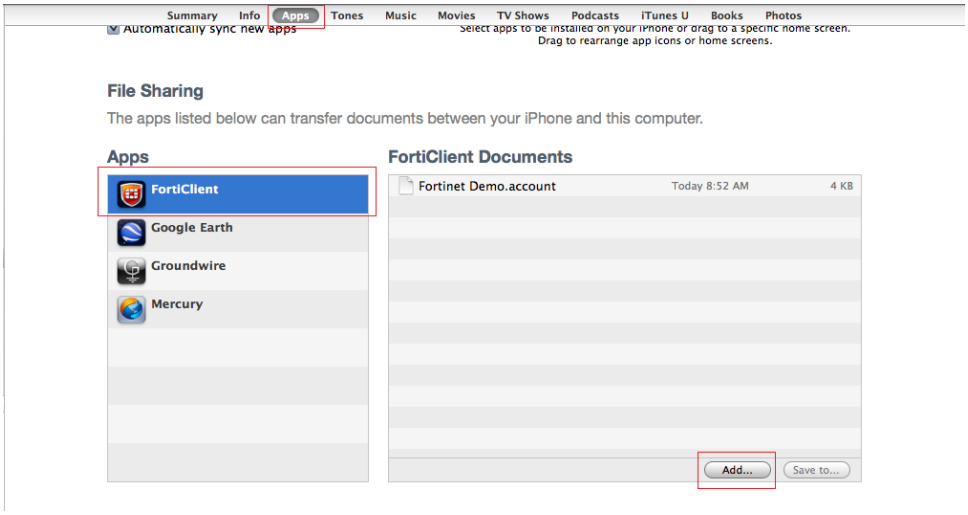
Figure 7: Certificate has been installed

Import client certificates to FortiClient using iTunes

To import certificates to the FortiClient application using iTunes, follow the steps listed below.

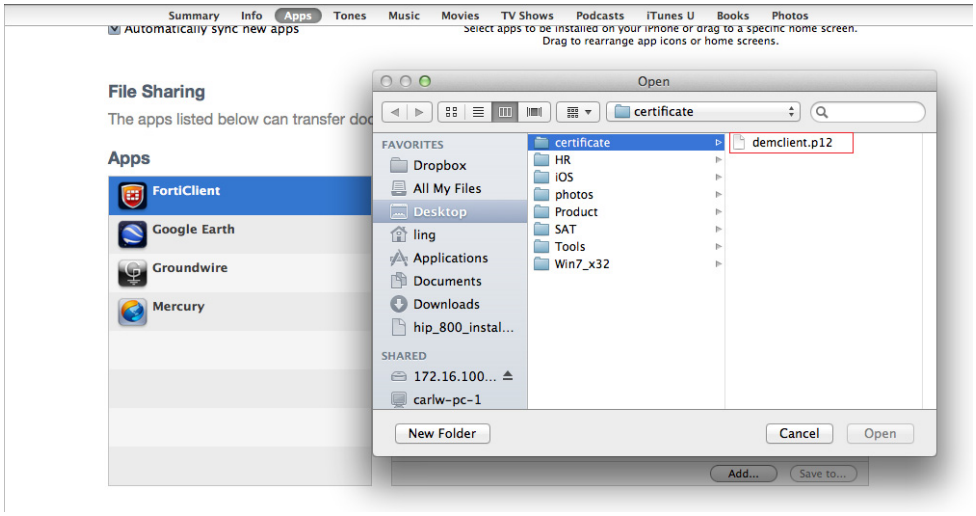
1. Open the iTunes program, and connect your iOS device.
2. Browse to the iOS device home screen page, and select *Apps*. Scroll down on the page to *File Sharing*, and select the FortiClient icon in the Apps column.

Figure 8: iOS device home screen



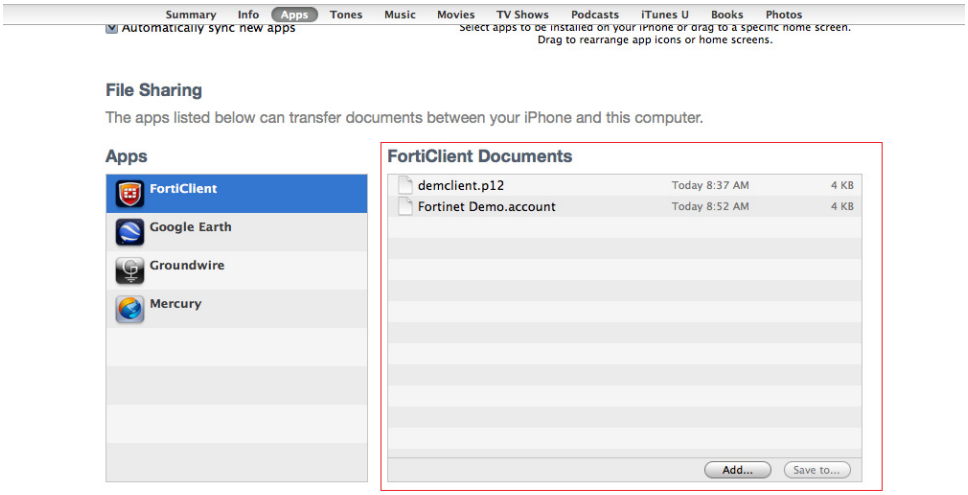
3. Select the *Add* button under *FortiClient Documents* and browse to you computers hard drive and locate the certificate file.

Figure 9: Browse to locate the certificate file



4. Select the certificate file and select *Open* to save it to the iTunes FortiClient document *File Sharing* directory.
5. Save to File Sharing directory, and sync the iOS device with iTunes

Figure 10: FortiClient Documents.



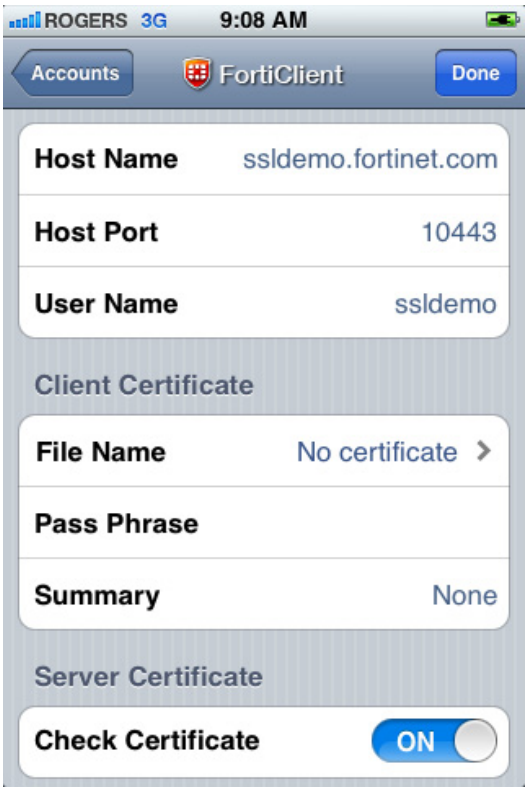
Configure client certificates imported to iTunes

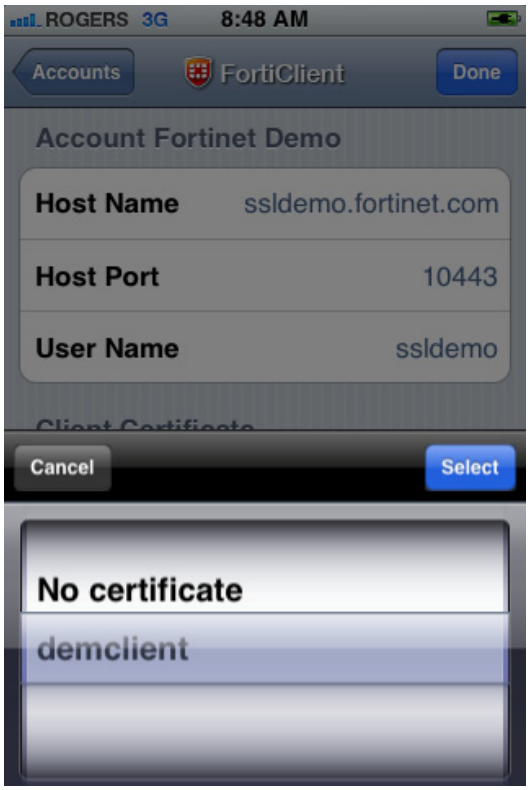
To configure certificates on the FortiClient application that have been imported using iTunes, follow the steps listed below.

1. Open the FortiClient application, select the account, under *Client Certificate* > *File Name*, browse for the certificate you added in iTunes. Select the certificate and then select Done to save the certificate to the FortiClient account.

You can associate a certificate to each FortiClient account.

Figure 11: Select the certificate.

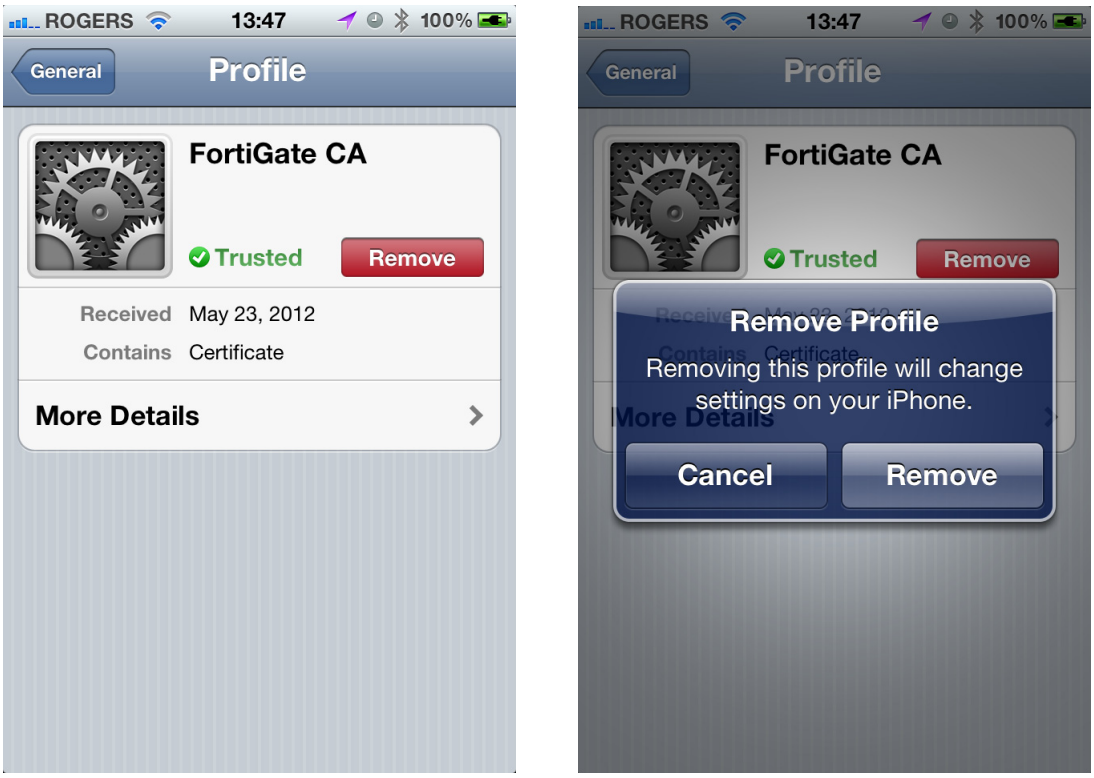




Certificate removal

To remove an installed certificate from your iOS device, go to *Settings* > *General* > *Profiles*. Select Remove to uninstall the certificate.

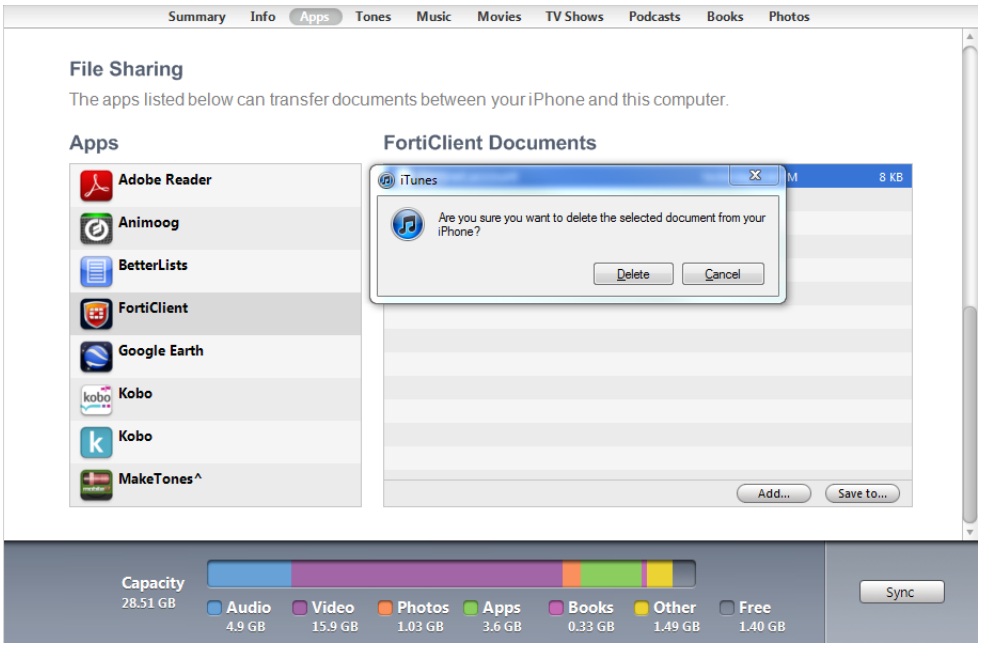
Figure 12: Remove certificate from iOS device



For client certificates added using iTunes, the certificate needs to be deleted from the FortiClient Document folder. To remove the certificate, follow the steps below.

1. Connect the iOS device to your computer and open the iTunes program.
2. Select the device name on the left menu pane, on the iTunes device home page select *Apps* > *File Sharing*.
3. Select the FortiClient app on the *Apps* menu, and then select the certificate file listed under FortiClient Documents. Use the delete key on your personal computer, and select Delete on the iTunes popup window to confirm the removal of the certificate from iTunes.

Figure 13: Delete the certificate file



iOS Configuration Utility

The iOS Configuration Utility is available from Apple for both Windows and Mac OS. Use the utility to create, maintain encrypt configuration profiles, track and install provisioning profiles, and authorized applications. The iOS Configuration Utility is available at the following links.

Windows

http://support.apple.com/downloads/iPhone_Configuration_Utility_2_0_for_Windows

Mac OS

http://support.apple.com/kb/DL1465